In the Claims:

Amend the claims as follows:

1. (Currently amended) A method for sending messages over secure communication links in networks, comprising:
providing at least a first terminal in communication with ~~being able to change its method of network access and at least one other~~ a second terminal ~~with one or more possible intermediate computers between the first terminal and the other terminal performing network address and/or other translations~~,
establishing a first secure communication link ~~being established~~ between an initial network address of the first terminal and ~~the~~ a network address of the ~~other~~ second terminal,
~~the link defining at least the addresses of the two terminals, and~~ the first terminal performing encapsulation of messages sent in the first ~~in said~~ secure communication link using a first encapsulation method, ~~to overcome network address and/or other translations made by said intermediate computers on the route, comprising:~~
~~a)~~ the first terminal moving from ~~said~~ the initial network address to a new network address,
~~b)~~ the first terminal sending an encapsulated request message, using the first encapsulation method, ~~from the first terminal~~ to the ~~other~~ second terminal to change communication between the first terminal and the second terminal from the first secure communication link to a second secure communication link extending ~~said secure connection to be~~ between the new network address of the first terminal and the network address of the second ~~other~~ terminal, the encapsulated request message ~~also~~ containing a description of the first encapsulation method performed by the first terminal,

the second terminal receiving the encapsulated request message,

the second terminal using the description of the first encapsulation method to ~~on the basis of which description the other terminal~~ detect~~s~~ translations of the encapsulated request message performed by ~~said~~ intermediate computers disposed en route between the first terminal and the second terminal,

~~c)~~ the ~~other~~ second terminal responding to the first terminal with a reply message, the reply message having ~~with~~ a description about detected translations made by ~~said possible~~ intermediate computers disposed between the new network address of the first terminal and the ~~other~~ network address of the second terminal and/or encapsulation methods supported by the ~~other~~ second terminal,

the first terminal receiving the reply message and the description about translation made by intermediate computers and encapsulation methods supported by the second terminal,

the first terminal selecting an encapsulation method to encapsulate a message based on the description of the reply message, and

~~d) thereafter~~ the first terminal sending the encapsulated message ~~from the first terminal~~ to the ~~other~~ second terminal ~~by using the information sent with said reply~~.

2. (Currently amended) The method of claim 1 wherein the method further comprises the second terminal detecting address translations performed by the intermediate computers and including a description of translated source and/or destination addresses in ~~description of~~ the reply message ~~include source and/or destination addresses on the basis of which the second receiving terminal detects address translations performed by intermediate computers~~.

3. (Currently amended) The method of claim 1 wherein the

description of the reply message has ~~of the message includes~~ information about encapsulation protocols, as well as source and destination transmission control protocol (TCP) or user datagram protocol (UDP) ports.

4. (Currently amended) The method of claim 3 wherein the method further comprises performing network address translation (NAT) traversal ~~is performed~~ by UDP encapsulation~~,~~ or TCP encapsulation ~~and/or by another encapsulation~~.

5. (Currently amended) The method of claim 1 wherein ~~after receiving of the request message by said other terminal sent in step c), the other terminal determines by~~ the method further comprises the second terminal examining the encapsulated request message to determine~~,~~ which translations and/or encapsulations are required in ~~the~~ traffic between the first terminal and the ~~other~~ second terminal.

6. (Currently amended) The method of claim 5 wherein the reply message ~~of step c)~~ contains information about the second secure communication link to be used between the new network address of the first terminal and ~~said other~~ the second terminal.

7. (Currently amended) The method of claim 6 wherein the information about the second secure communication link includes information about whether network address translation (NAT) traversal is ~~and/or other encapsulation should be~~ used.

8. (Currently amended) The method of claim 1 wherein the method further comprises ~~in step c)~~ the first terminal ~~compares~~ comparing the description~~s~~ of the request message with the description of the ~~respective~~ reply message~~s~~ and ~~sends~~ sending ~~all~~ subsequent messages from ~~this~~ the new network address based on the comparison of the descriptions

regarding which ~~on the basis of the comparison telling what~~ encapsulations, protocols and rules to use ~~should be used in the further communication~~.

9. (Currently amended) The method of claim 1 wherein the first secure communication link is formed by using an ~~the~~ Internet security protocol IPSec ~~protocol~~.

10. (Currently amended) The method of claim 9 wherein the reply message ~~in step d)~~ is sent by using IPSec and a network address translation (NAT) traversal that is updated to the new network address of the first terminal.

11. (Currently amended) The method of claim 1 wherein the reply message ~~in step d)~~ is sent without a network address translation (NAT) traversal in the first secure communication link when the description of the reply message corresponds to the description of the request message ~~the descriptions correspond to each other~~.

12. (Currently amended) The method of claim 1 wherein the method further comprises providing a the secure connection with ~~is~~ an Internet security protocol (IPSec) security association (SA).

13. (Currently amended) The method of claim 12 wherein the method further comprises using a key exchange mechanism that passes through a network address translation (NAT) ~~is used~~ when forming the IPSec SA.

14. (Currently amended) The method of claim 12 wherein ~~the~~ a key exchange mechanism ~~protocol~~ is an Internet key exchange (IKE) when ~~the~~ a network address translation (NAT) device supports ~~the~~ a user datagram protocol (UDP) ~~protocol~~.

15. (Currently amended) The method of claim 14 wherein ~~a~~ the key exchange mechanism is used when forming the IPSec SA and wherein several traversal mechanisms are used simultaneously to increase ~~the~~ a chance that at least one of the traversal mechanisms passes ~~them pass~~ through the NAT device.

16.(Previously presented) The method of claim 12 wherein a key exchange mechanism is performed when forming the IPSec SA in which a negotiation process is used to agree on protocols to be used in the further communication.

17. (Currently amended) The method of claim 12 wherein an encapsulation protocol is used in ~~the~~ a key exchange mechanism when forming the IPSec SA.

18. (Currently amended) The method of claim 1 wherein the network address of the ~~other~~ second terminal is ~~the~~ an end destination address of messages sent from the first terminal~~,~~ ~~in which~~ and using case transport or tunnel mode ~~is used~~ in the first and second secure ~~IPSec~~ communication links.

19. (Currently amended) The method of claim 1 wherein a ~~the~~ destination address of the message is ~~the~~ a network address of a host which is not the ~~other~~ second terminal~~, in which case~~ and using tunnel mode or transport mode together with a tunneling protocol ~~is used in the IPSec~~ the first and second secure communication links.

20. (Currently amended) The method of claim 1 wherein several request messages ~~of step b)~~ are sent, each request message being processed using a different traversal mechanism~~, where after the other terminal indicates~~ and the second terminal indicating in the reply message which encapsulation method~~s~~ is to be used ~~in the further communication~~.